УДК 004.4

О.В. Хейдер
Науковий керівник – Мелешко Є.В., канд. техн. наук, доцент
Кіровоградський національний технічний університет

Розробка програмного забезпечення ЕЦП для автентифікації користувачів у системах дистанційного навчання та тестування

У сучасних умовах збільшення кількості інформації, оброблюваної, переданої й збереженої в системах дистанційного навчання й тестування, привело до підвищення актуальності завдань:

− забезпечення конфіденційності, цілісності, незаперечення авторства електронного документа системи дистанційного навчання й тестування;

− створення захищеного системи дистанційного навчання й тестування;

− забезпечення високої швидкості обробки й підписання електронного документа системи дистанційного навчання й тестування.

У цей час основу забезпечення безпеки системи дистанційного навчання й тестування становлять системи електронного цифрового підпису (ЕЦП). Найбільше широко застосовуваним видом ЕЦП є індивідуальний підпис. Сучасні системи дистанційного навчання й тестування дозволяють обробляти й підписувати документ одночасно тільки одним користувачем, що збільшує час обробки й підписання документа, якщо його повинні підписати трохи користувачів. Отже, розмір ЕЦП збільшується пропорційно числу користувачів, що підписують електронний документ у кілька разів. При цьому процедура перевірки дійсності підпису має на увазі перевірку підписів всіх що підписали.

Крім того, варіант “один документ – один підпис” є не єдиним, необхідним на практиці. Зокрема, питання передачі документів від імені деякого колегіального органа або від імені сукупності суб'єктів роблять актуальним питання розробки систем ЕЦП на основі поняття колективного відкритого ключа. Ідея ЕЦП на основі відкритого колективного ключа полягає в тому, щоб побудувати протокол формування й перевірки підпису таким чином, що ЕЦП звичайного розміру буде підтверджувати дійсність деякого заданого електронного документа системи дистанційного навчання й тестування, підписаного кожним користувачем з деякого заданої безлічі користувачів.

В області теорії й практики розробки ЕЦП, як у нашій країні, так і за рубежем, видана велика кількість праць. З їхнього числа слід зазначити роботи ЭльГамаля Т., Шнорра К., Рабина М., Кобліца Н., Горбенко І.Д., Долгова В.І., Ростовцева А. Г., Черемушкина А. В., Молдовяна Н. А., Еремеева М. А., Маховенко Е. Б., і ін.

Створення методу формування й перевірки ЕЦП на основі колективного відкритого ключа дає можливість обробки й підписання документа одночасно декількома користувачами. При цьому розмір ЕЦП не збільшується, що дозволяє скоротити обсяг надлишкової інформації, необхідної для автентифікації електронних

документів і спростити протокол підтримки такого ЕЦП. Час на підписання документа залишається колишнім, як і при стандартній процедурі підпису, а час перевірки дійсності ЕЦП зменшується.

Таким чином, виявлена проблемна ситуація, обумовлена як протиріччя між необхідністю забезпечення дійсності й збереження цілісності інформації в системі дистанційного навчання й тестування при колективній обробці електронних документів і невідповідністю існуючих методів, алгоритмів і засобів організації захищеного документообігу сучасним вимогам захищеності, функціональності, а також оперативності.

Розрішення даної проблемної ситуації вимагає створення методу формування й перевірки електронного цифрового підпису на основі колективного відкритого ключа.

Метою магістерської роботи є розробка програмного забезпечення ЕЦП для автентифікації користувачів у системах дистанційного навчання та тестування.

Для досягнення поставленої мети вирішувалося наукове завдання побудови схем електронного цифрового підпису на основі колективного відкритого ключа.

Досягнення поставленої мети й рішення наукового завдання зажадало рішення наступних часткових завдань досліджень:

1. Проведення аналізу сучасних методів і засобів захисту систем дистанційного навчання й тестування.

2. Здійснення вибору системи електронного цифрового підпису як основного механізму забезпечення оперативного захищеного системи дистанційного навчання й тестування.

3. Розробки методу формування й перевірки електронного цифрового підпису на основі відкритого колективного ключа.

4. Розробки алгоритму вибору параметрів електронного цифрового підпису на основі відкритого колективного ключа.

5. Розробки методики організації захищеної системи дистанційного навчання й тестування.

6. Розробки програмного комплексу по реалізації електронного цифрового підпису на основі відкритого колективного ключа й рекомендації з її впровадження в систему захищеного дистанційного навчання й тестування (системи захищеного дистанційного навчання й тестування).

Об'єктом дослідження є процес реалізації системи дистанційного навчання й тестування

Предмет – методи створення й перевірки електронного цифрового підпису при організації системи дистанційного навчання й тестування.

Список літератури

1. "Дистанционные методы обучения. Состояние, проблемы, перспективы." // Дайджест педагогічних ідей та технологій "Школа – парк". – 2001. – № 3-4. – С. 81 – 103
2. Трохименко В. Дистанційне навчання педагогічних працівників: досвід і проблеми// Післядипломна освіта в Україні. – 2004. – С. 29 – 32.
3. Ахаян А.А. Виртуальный педагогический вуз. Теория становления. – СПб.: Изд-во "Корифей", 2001. – 170 с.
4. Зайченко Т.П. Основы дистанционного обучения: Теоретико-практический базис: Учебное пособие. – СПб.: Изд-во РГПУ им. А.И. Герцена, 2004. – 167 с.